

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Hideo SHIMIZU, et al.

GAU:

SERIAL NO: NEW APPLICATION

EXAMINER:

FILED: HERewith

FOR: POLYNOMIAL INVERSE COMPUTING APPARATUS, MULTIPLIER APPARATUS AND
POLYNOMIAL INVERSE COMPUTING METHOD

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of 35 U.S.C. §119(e):
Application No. Date Filed

☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

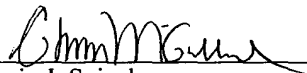
<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
Japan	2002-287860	September 30, 2002

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
- ☐ (B) Application Serial No.(s)
☐ are submitted herewith
☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.


Marvin J. Spivak

Registration No. 24,913
C. Irvin McClelland
Registration Number 21,124

Customer Number

22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年 9月30日

出 願 番 号

Application Number:

特願2002-287860

[ST.10/C]:

[JP2002-287860]

出 願 人

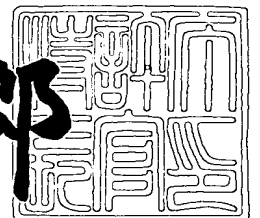
Applicant(s):

株式会社東芝

2003年 2月21日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田信一郎



出証番号 出証特2003-3009707

【書類名】 特許願

【整理番号】 A000202891

【提出日】 平成14年 9月30日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 15/00

【発明の名称】 逆元計算装置及び逆元計算方法

【請求項の数】 11

【発明者】

【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝研
究開発センター内

【氏名】 清水 秀夫

【発明者】

【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝研
究開発センター内

【氏名】 新保 淳

【特許出願人】

【識別番号】 000003078

【氏名又は名称】 株式会社 東芝

【代理人】

【識別番号】 100058479

【弁理士】

【氏名又は名称】 鈴江 武彦

【電話番号】 03-3502-3181

【選任した代理人】

【識別番号】 100084618

【弁理士】

【氏名又は名称】 村松 貞男

【選任した代理人】

【識別番号】 100068814

【弁理士】

【氏名又は名称】 坪井 淳

【選任した代理人】

【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【弁理士】

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

【選任した代理人】

【識別番号】 100070437

【弁理士】

【氏名又は名称】 河井 将次

【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 逆元計算装置及び逆元計算方法

【特許請求の範囲】

【請求項 1】

第 1 乃至第 6 のレジスタと、左シフト回路と、排他的論理和回路と、標数 2 の拡大体での 2 倍演算を施す 2 倍演算回路と、標数 2 の拡大体での $1/2$ 倍演算を施す $1/2$ 倍演算回路と、レジスタの内容が 0 か否か判定する判定回路と、レジスタの内容をデクリメントするデクリメント回路と、レジスタの内容をインクリメントするインクリメント回路と、それらを制御する制御回路とを用いて構成したことを特徴とする逆元計算装置。

【請求項 2】

初期値として除数を格納する第 1 のレジスタと、

初期値として法を格納し、所定の場合に前記第 1 のレジスタの内容を保持する第 2 のレジスタと、

初期値として被除数を格納する第 3 のレジスタと、

初期値として 0 を格納し、所定の場合に前記第 3 のレジスタの内容を保持し、最終的に計算結果を保持する第 4 のレジスタと、

初期値として法のビット数を格納する第 5 のレジスタと、

初期値として 0 を格納する第 6 のレジスタと、

所定の場合に前記第 1 のレジスタを左シフトする左シフト回路と、

所定の場合に前記第 1 のレジスタと前記第 2 のレジスタの排他的論理和を求めて該第 1 のレジスタへ出力する第 1 の排他的論理和回路と、

所定の場合に前記第 3 のレジスタに対して標数 2 の拡大体での 2 倍演算を施す 2 倍演算回路と、

所定の場合に前記第 4 のレジスタに対して標数 2 の拡大体での $1/2$ 倍演算を施す $1/2$ 倍演算回路と、

所定の場合に前記第 3 のレジスタと前記第 4 のレジスタの排他的論理和を求め該第 3 のレジスタへ出力する第 2 の排他的論理和回路と、

所定の場合に前記第 5 のレジスタが 0 か否か判定する第 1 の判定回路と、

所定の場合に前記第 5 のレジスタをデクリメントする第 1 のデクリメント回路と、

所定の場合に前記第 6 のレジスタが 0 か否かを判定する第 2 の判定回路と、

所定の場合に前記第 6 のレジスタをデクリメントする第 2 のデクリメント回路と、

所定の場合に前記第 6 のレジスタをインクリメントするインクリメント回路とを備えたことを特徴とする逆元計算装置。

【請求項 3】

第 1 の状態においては、前記第 1 のレジスタの最上位ビットが 1 でない限りは、前記第 1 のレジスタを前記左シフト回路により左シフトし、前記第 3 のレジスタを前記 2 倍演算回路により 2 倍し、前記第 5 のレジスタを前記第 1 のデクリメント回路により 1 だけデクリメントし、前記第 6 のレジスタを前記インクリメント回路により 1 だけインクリメントする一連の処理を繰り返し行い、前記第 1 のレジスタの最上位ビットが 1 であるときは、第 2 の状態に状態遷移し、

第 2 の状態においては、前記第 1 のレジスタ及び前記第 2 のレジスタにそれぞれ前記第 1 の排他的論理和回路の出力及び該第 1 のレジスタの内容を格納するとともに、前記第 3 のレジスタ及び前記第 4 のレジスタにそれぞれ前記第 2 の排他的論理和回路の出力及び該第 3 のレジスタの内容を格納し、その後第 3 の状態に状態遷移し、

第 3 の状態においては、前記第 2 の判定回路により前記第 6 のレジスタが 0 でないと判定される限り、まず、前記第 1 のレジスタの最上位ビットが 1 である場合にのみ、該第 1 のレジスタに前記第 1 の排他的論理和回路の出力を格納するとともに、前記第 3 のレジスタに前記第 2 の排他的論理和回路の出力を格納し、次いで、前記第 6 のレジスタを前記第 2 のデクリメント回路により 1 だけデクリメントし、前記第 1 のレジスタを前記左シフト回路により左シフトし、前記第 4 のレジスタを前記 1 / 2 倍演算回路により 1 / 2 倍する一連の処理を繰り返し行い、前記第 2 の判定回路により前記第 6 のレジスタが 0 になったと判定されたときは、前記第 1 の判定回路により前記第 5 のレジスタが 0 でないと判定されたならば、前記第 1 の状態に状態遷移し、0 であると判定されたならば、前記第 4 レジ

スタの内容を結果として出力することを特徴とする請求項 2 に記載の逆元計算装置。

【請求項 4】

前記 2 倍演算回路は、前記第 3 のレジスタの最上位ビットが 1 である場合には、前記第 3 のレジスタを 1 ビットだけ左シフトした後に、前記法との排他的論理和を取り、前記第 3 のレジスタの最上位ビットが 0 である場合には、前記第 3 のレジスタを 1 ビットだけ左シフトするものであることを特徴とする請求項 1 ないし 3 のいずれか 1 項に記載の逆元計算装置。

【請求項 5】

前記 1 / 2 倍演算回路は、前記第 4 のレジスタの最下位ビットが 1 である場合には、前記法との排他的論理和を取った後に、1 ビットだけ右シフトし、前記第 4 のレジスタの最下位ビットが 0 である場合には、前記第 4 のレジスタを 1 ビットだけ右シフトするものであることを特徴とする請求項 1 ないし 4 のいずれか 1 項に記載の逆元計算装置。

【請求項 6】

前記第 5 のレジスタをワンホットカウンタで実現したことを特徴とする請求項 1 ないし 5 のいずれか 1 項に記載の逆元計算装置。

【請求項 7】

前記第 6 のレジスタをワンホットカウンタで実現したことを特徴とする請求項 1 ないし 6 のいずれか 1 項に記載の逆元計算装置。

【請求項 8】

請求項 1 ないし 7 のいずれか 1 項に記載の前記第 1 及び第 3 乃至第 5 のレジスタ、前記左シフト回路、前記第 1 又は第 2 の排他的論理和回路、前記 2 倍演算回路、前記第 1 又は第 2 の判定回路並びに前記第 1 又は第 2 のデクリメント回路を、前記逆元計算装置と共用し、

前記第 1 及び第 3 乃至第 5 のレジスタに初期値としてそれぞれ乗数、0、被乗数、法のビット数を格納し、

前記第 1 又は第 2 の判定回路により前記第 5 のレジスタが 0 でないと判定される限り、前記第 5 のレジスタを前記第 1 又は第 2 のデクリメント回路により 1 だ

けデクリメントし、前記第3のレジスタを前記2倍演算回路により2倍し、前記第1のレジスタを前記左シフト回路により左シフトし、前記第1のレジスタの最上位ビットが1である場合にのみ、前記第3のレジスタに、該第3のレジスタと前記第4のレジスタを入力とする前記第1又は第2の排他的論理和回路の出力を格納する一連の処理を繰り返し行い、前記第1又は第2の判定回路により前記第5のレジスタが0になったと判定されたときは、前記第3レジスタの内容を結果として出力することを特徴とする乗算装置。

【請求項9】

第1乃至第6のレジスタに初期値としてそれぞれ除数、法、被除数、0、法のビット数及び0を格納し、

第1の状態においては、前記第1のレジスタの最上位ビットが1でない限りは、前記第1のレジスタを左シフト回路により左シフトし、前記第3のレジスタに対して2倍演算回路により標数2の拡大体での2倍演算を施し、前記第5のレジスタを第1のデクリメント回路により1だけデクリメントし、前記第6のレジスタをインクリメント回路により1だけインクリメントする一連の処理を繰り返し行い、前記第1のレジスタの最上位ビットが1であるときは、第2の状態に状態遷移し、

第2の状態においては、前記第1のレジスタ及び前記第2のレジスタにそれぞれ該第1のレジスタと該第2のレジスタを入力とする第1の排他的論理和回路の出力及び該第1のレジスタの内容を格納するとともに、前記第3のレジスタ及び前記第4のレジスタにそれぞれ該第3のレジスタと該第4のレジスタを入力とする第2の排他的論理和回路の出力及び該第3のレジスタの内容を格納し、その後第3の状態に状態遷移し、

第3の状態においては、前記第6のレジスタが0でない限り、まず、前記第1のレジスタの最上位ビットが1である場合にのみ、該第1のレジスタに前記第1の排他的論理和回路の出力を格納するとともに、前記第3のレジスタに前記第2の排他的論理和回路の出力を格納し、次いで、前記第6のレジスタを第2のデクリメント回路により1だけデクリメントし、前記第1のレジスタを前記左シフト回路により左シフトし、前記第4のレジスタに対して1/2倍演算回路により標

数 2 の拡大体での $1/2$ 倍演算を施す一連の処理を繰り返し行い、前記第 6 のレジスタが 0 になったときは、前記第 5 のレジスタが 0 でないならば、前記第 1 の状態に状態遷移し、0 であるならば、前記第 4 レジスタの内容を結果として出力することを特徴とする逆元計算方法。

【請求項 1 0】

前記 2 倍演算では、前記第 3 のレジスタの最上位ビットが 1 である場合には、前記第 3 のレジスタを 1 ビットだけ左シフトした後に、前記法との排他的論理和を取り、前記第 3 のレジスタの最上位ビットが 0 である場合には、前記第 3 のレジスタを 1 ビットだけ左シフトすることを特徴とする請求項 9 に記載の逆元計算方法。

【請求項 1 1】

前記 $1/2$ 倍演算では、前記第 4 のレジスタの最下位ビットが 1 である場合には、前記法との排他的論理和を取った後に、1 ビットだけ右シフトし、前記第 4 のレジスタの最下位ビットが 0 である場合には、前記第 4 のレジスタを 1 ビットだけ右シフトすることを特徴とする請求項 9 または 1 0 に記載の逆元計算方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、V L S I 実装に適した標数 2 のガロア体での逆元計算装置及び逆元計算方法に関する。

【0 0 0 2】

【従来の技術】

標数 2 のガロア体は符号理論や楕円曲線暗号等の様々な工業分野に応用されている。標数 2 のガロア体の元の逆元の計算は標数 2 の楕円曲線上の有理点の加算に必要とされる演算である。

【0 0 0 3】

任意の体の元の逆元を計算するアルゴリズムとしては、拡張ユークリッドアルゴリズムが知られている。しかし、拡張ユークリッドアルゴリズムは乗算と除算を必要とするため、ハードウェアで実装した際には実行ステップ数や回路規模が

大きくなるという問題があった。

【0 0 0 4】

1 9 8 7 年に S t e i n は乗算と除算がいらぬ拡張ユークリッドアルゴリズムの改良を提案している。この改良により、標数 2 のガロア体の逆元は、シフト演算、排他的論理和、2 つの多項式の最高次数の比較回路、多項式が定数であるかの判定回路及び制御回路により構成できる。

【0 0 0 5】

一般に V L S I の性能は、実行サイクル数（レイテンシ）、回路規模、回路遅延の 3 つにより決まる。法多項式の最高次数を m とすると、S t e i n のアルゴリズムではレイテンシは $2m$ ステップであり、理論的にこれ以上の高速化は望めない。回路規模は $O(m)$ であり、回路遅延は $O(\log m)$ である。上で列挙したうち、2 つの多項式の最高次数の比較回路と多項式が定数であるかの判定回路の 2 つが回路規模と回路遅延の両方を大きくしている。楕円曲線暗号への応用では、 m は数百程度である。

【0 0 0 6】

その他、種々のガロア体逆元演算の高速化が提案されている（例えば、下記特許文献 1 ～ 4 参照）。

【0 0 0 7】

【特許文献 1】

特開 2 0 0 0 - 0 4 7 8 3 3 号公報

【0 0 0 8】

【特許文献 2】

特開 2 0 0 0 - 3 1 5 2 0 1 号公報

【0 0 0 9】

【特許文献 3】

特開 2 0 0 0 - 3 2 2 2 8 0 号公報

【0 0 1 0】

【特許文献 4】

特開 2 0 0 2 - 0 2 3 9 9 9 号公報

【 0 0 1 1 】

【発明が解決しようとする課題】

従来知られていた標数 2 のガロア体での逆元計算アルゴリズムである S t e i n のアルゴリズムでは、V L S I 化した際に回路規模と回路遅延が大きくなる問題があった。

【 0 0 1 2 】

本発明は、上記事情を考慮してなされたもので、標数 2 のガロア体での逆元計算アルゴリズムを V L S I 化した際、回路規模や回路遅延を従来よりも小さく抑えることができる逆元計算装置及び逆元計算方法を提供することを目的とする。

【 0 0 1 3 】

また、本発明は、標数 2 のガロア体での逆元計算アルゴリズムを V L S I 化した際、逆元計算装置と大部分の部品を共通に利用することができる乗算装置を提供することを目的とする。

【 0 0 1 4 】

【課題を解決するための手段】

本発明に係る逆元計算装置は、第 1 乃至第 6 のレジスタと、左シフト回路と、排他的論理和回路と、標数 2 の拡大体での 2 倍演算を施す 2 倍演算回路と、標数 2 の拡大体での $1/2$ 倍演算を施す $1/2$ 倍演算回路と、レジスタの内容が 0 か否か判定する判定回路と、レジスタの内容をデクリメントするデクリメント回路と、レジスタの内容をインクリメントするインクリメント回路と、それらを制御する制御回路とを用いて構成したことを特徴とする。

【 0 0 1 5 】

また、本発明に係る逆元計算装置は、初期値として除数を格納する第 1 のレジスタと、初期値として法を格納し、所定の場合に前記第 1 のレジスタの内容を保持する第 2 のレジスタと、初期値として被除数を格納する第 3 のレジスタと、初期値として 0 を格納し、所定の場合に前記第 3 のレジスタの内容を保持し、最終的に計算結果を保持する第 4 のレジスタと、初期値として法のビット数を格納する第 5 のレジスタと、初期値として 0 を格納する第 6 のレジスタと、所定の場合に前記第 1 のレジスタを左シフトする左シフト回路と、所定の場合に前記第 1 の

レジスタと前記第 2 のレジスタの排他的論理和を求めて該第 1 のレジスタへ出力する第 1 の排他的論理和回路と、所定の場合に前記第 3 のレジスタに対して標数 2 の拡大体での 2 倍演算を施す 2 倍演算回路と、所定の場合に前記第 4 のレジスタに対して標数 2 の拡大体での $1/2$ 倍演算を施す $1/2$ 倍演算回路と、所定の場合に前記第 3 のレジスタと前記第 4 のレジスタの排他的論理和を求め該第 3 のレジスタへ出力する第 2 の排他的論理和回路と、所定の場合に前記第 5 のレジスタが 0 か否かを判定する第 1 の判定回路と、所定の場合に前記第 5 のレジスタをデクリメントする第 1 のデクリメント回路と、所定の場合に前記第 6 のレジスタが 0 か否かを判定する第 2 の判定回路と、所定の場合に前記第 6 のレジスタをデクリメントする第 2 のデクリメント回路と、所定の場合に前記第 6 のレジスタをインクリメントするインクリメント回路とを備えたことを特徴とする。

【0016】

好ましくは、第 1 の状態においては、前記第 1 のレジスタの最上位ビットが 1 でない限りは、前記第 1 のレジスタを前記左シフト回路により左シフトし、前記第 3 のレジスタを前記 2 倍演算回路により 2 倍し、前記第 5 のレジスタを前記第 1 のデクリメント回路により 1 だけデクリメントし、前記第 6 のレジスタを前記インクリメント回路により 1 だけインクリメントする一連の処理を繰り返し行い、前記第 1 のレジスタの最上位ビットが 1 であるときは、第 2 の状態に状態遷移し、第 2 の状態においては、前記第 1 のレジスタ及び前記第 2 のレジスタにそれぞれ前記第 1 の排他的論理和回路の出力及び該第 1 のレジスタの内容を格納するとともに、前記第 3 のレジスタ及び前記第 4 のレジスタにそれぞれ前記第 2 の排他的論理和回路の出力及び該第 3 のレジスタの内容を格納し、その後第 3 の状態に状態遷移し、第 3 の状態においては、前記第 2 の判定回路により前記第 6 のレジスタが 0 でないと判定される限り、まず、前記第 1 のレジスタの最上位ビットが 1 である場合にのみ、該第 1 のレジスタに前記第 1 の排他的論理和回路の出力を格納するとともに、前記第 3 のレジスタに前記第 2 の排他的論理和回路の出力を格納し、次いで、前記第 6 のレジスタを前記第 2 のデクリメント回路により 1 だけデクリメントし、前記第 1 のレジスタを前記左シフト回路により左シフトし、前記第 4 のレジスタを前記 $1/2$ 倍演算回路により $1/2$ 倍する一連の処理

を繰り返し行い、前記第 2 の判定回路により前記第 6 のレジスタが 0 になったと判定されたときは、前記第 1 の判定回路により前記第 5 のレジスタが 0 でないと判定されたならば、前記第 1 の状態に状態遷移し、0 であると判定されたならば、前記第 4 レジスタの内容を結果として出力するようにしてもよい。

【 0 0 1 7 】

また、本発明に係る乗算装置は、請求項 1 ないし 7 のいずれか 1 項に記載の前記第 1 及び第 3 乃至第 5 のレジスタ、前記左シフト回路、前記第 1 又は第 2 の排他的論理和回路、前記 2 倍演算回路、前記第 1 又は第 2 の判定回路並びに前記第 1 又は第 2 のデクリメント回路を、前記逆元計算装置と共用し、前記第 1 及び第 3 乃至第 5 のレジスタに初期値としてそれぞれ乗数、0、被乗数、法のビット数を格納し、前記第 1 又は第 2 の判定回路により前記第 5 のレジスタが 0 でないと判定される限り、前記第 5 のレジスタを前記第 1 又は第 2 のデクリメント回路により 1 だけデクリメントし、前記第 3 のレジスタを前記 2 倍演算回路により 2 倍し、前記第 1 のレジスタを前記左シフト回路により左シフトし、前記第 1 のレジスタの最上位ビットが 1 である場合にのみ、前記第 3 のレジスタに、該第 3 のレジスタと前記第 4 のレジスタを入力とする前記第 1 又は第 2 の排他的論理和回路の出力を格納する一連の処理を繰り返し行い、前記第 1 又は第 2 の判定回路により前記第 5 のレジスタが 0 になったと判定されたときは、前記第 3 レジスタの内容を結果として出力することを特徴とする。

【 0 0 1 8 】

また、本発明に係る逆元計算方法は、第 1 乃至第 6 のレジスタに初期値としてそれぞれ除数、法、被除数、0、法のビット数及び 0 を格納し、第 1 の状態においては、前記第 1 のレジスタの最上位ビットが 1 でない限りは、前記第 1 のレジスタを左シフト回路により左シフトし、前記第 3 のレジスタに対して 2 倍演算回路により標数 2 の拡大体での 2 倍演算を施し、前記第 5 のレジスタを第 1 のデクリメント回路により 1 だけデクリメントし、前記第 6 のレジスタをインクリメント回路により 1 だけインクリメントする一連の処理を繰り返し行い、前記第 1 のレジスタの最上位ビットが 1 であるときは、第 2 の状態に状態遷移し、第 2 の状態においては、前記第 1 のレジスタ及び前記第 2 のレジスタにそれぞれ該第 1 の

レジスタと該第2のレジスタを入力とする第1の排他的論理和回路の出力及び該第1のレジスタの内容を格納するとともに、前記第3のレジスタ及び前記第4のレジスタにそれぞれ該第3のレジスタと該第4のレジスタを入力とする第2の排他的論理和回路の出力及び該第3のレジスタの内容を格納し、その後に第3の状態に状態遷移し、第3の状態においては、前記第6のレジスタが0でない限り、まず、前記第1のレジスタの最上位ビットが1である場合にのみ、該第1のレジスタに前記第1の排他的論理和回路の出力を格納するとともに、前記第3のレジスタに前記第2の排他的論理和回路の出力を格納し、次いで、前記第6のレジスタを第2のデクリメント回路により1だけデクリメントし、前記第1のレジスタを前記左シフト回路により左シフトし、前記第4のレジスタに対して1/2倍演算回路により標数2の拡大体での1/2倍演算を施す一連の処理を繰り返し行い、前記第6のレジスタが0になったときは、前記第5のレジスタが0でないならば、前記第1の状態に状態遷移し、0であるならば、前記第4レジスタの内容を結果として出力することを特徴とする。

【0019】

なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。

また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムとしても成立し、該プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【0020】

本発明によれば、標数2のガロア体での逆元計算アルゴリズムをVLSI化した際、回路規模や回路遅延を従来よりも小さく抑えることができるようになる。例えば、法となる多項式の最高次数を m としたとき、従来方法の `circuit depth` は、 $\log m$ であったが、本発明によれば、 $\log \log m$ に削減することができる。

【0021】

また、本発明によれば、全てのシフト操作が、1ビット固定シフトとなる、という利点が得られる。

【0022】

また、本発明によれば、逆元計算装置と乗算装置とで大部分の部品を共通に利用することができる。

【0023】

【発明の実施の形態】

以下、図面を参照しながら発明の実施の形態を説明する。

【0024】

法をGとして、GF(2)の拡大体でのAの逆元の計算を行うためのアルゴリズムを以下に示す。

【0025】

法G(Gはm次多項式), m, 除数a(aは次数がmより小さい多項式), 非除数b(bは次数がmより小さい多項式)は、入力として与える。

【0026】

初期値として、下記のようにする。

$A = a$ (Aはm次多項式)

$B = b$ (Bはm次多項式)

$C = G$ (Cはm次多項式)

$D = 0$ (Dはm次多項式)

$n = 0$ (nはm以下の整数を表せる変数)

なお、本アルゴリズムは、アルゴリズムが完了したときのDが、演算結果 $A^{-1} \cdot B$ を与えるものである。従って、Aの逆元の計算の場合には、Bの初期値すなわちbを1とする。本アルゴリズムによって、逆元計算だけしか行わない場合には、bを入力とせず、Bの初期値を1に固定してもよい。

【0027】

本アルゴリズムの記述は以下のとおりである。なお、下記のアルゴリズムにおいて、 $msb(A)$ は、Aの最高次の係数を意味する。また、 $left_shift(A)$ は、多項式AにXを掛けて X^m で割った剰余を意味する。また、t

$wice(B)$ は、多項式 B に X を掛けて法多項式 G で割った剰余を意味する。
 また、 $half(D)$ は、多項式 D に $1/X$ を掛けて法多項式 G で割った剰余を意味する。

【 0 0 2 8 】

<逆元計算アルゴリズム 1>

G, m, a, b の入力

A, B, C, D, n の初期化

while $m \neq 0$

 // step 1

 while $msb(A) = 0$

$m \leftarrow m-1;$

$n \leftarrow n+1;$

$A \leftarrow left_shift(A);$

$B \leftarrow twice(B);$

 wend

 // step 2

$(A, C) \leftarrow (A \text{ xor } C, A);$

$(B, D) \leftarrow (B \text{ xor } D, B);$

 // step 3

 while $n \neq 0$

 if $msb(A) = 1$ then $(A, B) \leftarrow (A \text{ xor } C, B \text{ xor } D)$

$n \leftarrow n-1$

$A \leftarrow left_shift(A)$

$D \leftarrow half(D)$

 wend

wend

D を出力

<逆元計算アルゴリズム 1>

以上のアルゴリズムの記述をフローチャートの形で表したのが図 1 である。

【0029】

ここで、 $m-1$ 次多項式を、図2のように係数を並べて表現することにする。
 例えば、法を x^4+x+1 とすると、 x^4+x+1 は (1,0,0,1,1) で表され、 $x+1$ は (0,0,0,1,1) で表され、 x^3+x^2+1 は (0,1,1,1,0) で表され、0 は (0,0,0,0,0) で表され、1 は (0,0,0,0,1) で表される。

【0030】

この場合、`left_shift (A)` は、図3のように表現できる。

また、`twice (A)` は、図4のように表現できる。なお、ステップ S12、S13 の $A \ll 1$ は、A を左に1ビットだけシフトすることを表す。

また、`half (A)` は、図5のように表現できる。なお、ステップ S15、S16 の $A \gg 1$ は、A を右に1ビットだけシフトすることを表す。

【0031】

図6に、法 $G = x^4+x+1$ とし、 $a = x+1$ としたときの a の逆元を求める場合、すなわち $(x+1)^{-1} \bmod (x^4+x+1)$ を求める場合における、上記アルゴリズムの実行中の途中結果を示す（なお、この場合、 $b=1$ である）。

【0032】

ここで、法 $G = x^4+x+1$ であるので、 $m=4$ となる。よって、 $C=10011$ となる。また、除数 $a = x+1$ であり、 $m=4$ であるので、A の初期値は、 00011 とする。被除数 $b=1$ であり、 $m=4$ であるので、B の初期値は、 0001 とする。また、D の初期値は 00000 、 n の初期値は0である。

【0033】

本具体例の場合、D の最終的な値は、 01110 であるので、求める逆元は、 x^3+x^2+1 となる。

【0034】

図7に、上記アルゴリズムをハードウェア化した際の構成を示す。

【0035】

本アルゴリズムをハードウェア化した場合、この構成は、第1のレジスタA（図中、1）、第2のレジスタC（図中、2）、第3のレジスタB（図中、3）、

第4のレジスタD（図中、4）、第5のレジスタm（図中、5）、第6のレジスタn（図中、6）の6個のレジスタを持つ。また、図中の7～16の各回路を持つ。また、各レジスタや各回路の制御を行う制御回路（図示せず）を持つ。

【0036】

レジスタAは、左シフト回路8と、レジスタCとの排他的論理和回路7とに接続されており、制御回路（図示せず）に対して最上位ビット（図中、msb）を出力する。

【0037】

レジスタCは、レジスタAを入力として、レジスタAとの排他的論理和回路7に出力として接続している。

【0038】

レジスタBは、標数2の拡大体での2倍演算回路（twice）10と、レジスタDとの排他的論理和回路9とに接続している。

【0039】

レジスタDは、レジスタBと、標数2の拡大体での1/2倍演算回路（half）11と、レジスタBとの排他的論理和回路9に接続している。

【0040】

レジスタmは、デクリメント回路13と、0か否かを判定する判定回路12とに接続している。

【0041】

レジスタnは、インクリメント回路16と、デクリメント回路15と、0か否かを判定する判定回路14とに接続している。

【0042】

なお、レジスタA～Dは、楕円曲線暗号では数百ビット程度を格納でき、レジスタm、nは、数百程度の値が格納できるビット数を持つ。レジスタA～Dの長さが200ビット程度なら、レジスタm、nは8ビットあれば十分である。

【0043】

以上の構成でのクリティカルパスは、レジスタm、nのインクリメント回路とデクリメント回路であり、 $O(\log \log m)$ 段となる。

【0044】

このような構成において、前述したアルゴリズム（逆元計算アルゴリズム1）を実行する。すなわち、パラメータの入力、変数の初期化を行った後、第1の状態（step 1）においては、レジスタAの最上位ビットが1でない限りは、レジスタAを左シフトし、レジスタBを標数2の拡大体で2倍し、レジスタmの内容を1減らし、レジスタnの内容を1増やすことを繰り返し行うとともに、レジスタAの最上位ビットが1であるときは、第2の状態（step 2）に状態遷移する。

【0045】

第2の状態（step 2）においては、レジスタAに、レジスタAの内容とレジスタCの内容の排他的論理和を、レジスタCに、レジスタAの内容を、それぞれ格納し、また、レジスタBに、レジスタBの内容とレジスタDの内容の排他的論理和を、レジスタDに、レジスタBの内容を、それぞれ格納して、第3の状態（step 3）に状態遷移する。

【0046】

第3の状態（step 3）においては、レジスタnの内容が0でない限り、まず、レジスタAの最上位ビットが1である場合は、レジスタAに、レジスタCの内容を排他的論理和で加え、かつ、レジスタBに、レジスタDの内容を排他的論理和で加え、他方、レジスタAの最上位ビットが0である場合は、何もしない。次いで、レジスタnの内容を1減らし、レジスタAを左シフトし、レジスタDを標数2の拡大体で1/2倍することを、繰り返し行うとともに、レジスタnの内容が0になった場合は、レジスタmの内容が0でないならば、第1の状態（step 1）に状態遷移し、0であるならば、レジスタDの内容を結果として出力する。

【0047】

図8に、上記アルゴリズムをハードウェア化した際の状態遷移図を示す。

【0048】

初期状態は、step 1であり、msb(A)が0の間step 1に留まる。

【0049】

$msb(A)$ が 1 になると、step 2 に状態遷移し、step 2 からは、無条件に step 3 に状態遷移する。

【 0 0 5 0 】

n が 0 でない間、step 3 に留まり、 n が 0 になった際には、 m の値により、 m が 0 でないときは step 1 に戻り、 m が 0 であるときは終了する。

【 0 0 5 1 】

以上説明してきたように、本実施形態によれば、標数 2 のガロア体での逆元計算アルゴリズムを VLSI 化した際、回路規模や回路遅延を従来よりも小さく抑えることができるようになる。

【 0 0 5 2 】

例えば、法となる多項式の最高次数を m としたとき、従来方法の circuit depth は、 $\log m$ であったが、本実施形態によれば、 $\log \log m$ に削減することができる。

【 0 0 5 3 】

また、本実施形態では、全てのシフト操作が、1 ビット固定シフトとなる、という利点を得られる。

【 0 0 5 4 】

ここで、図 9 に、図 7 の本アルゴリズムをハードウェア化した際の構成と、大部分の部品を共通に利用できる乗算器の構成を示す。この場合、逆元計算装置と、4 つのレジスタ、および、1 つずつの左シフト回路、排他的論理和回路、2 倍演算回路、判定回路、デクリメント回路を共通に利用できる。例えば、図 7 の逆元計算装置と、レジスタ A、左シフト回路 8、レジスタ B、レジスタ D、排他的論理和回路 9、2 倍演算回路 10、レジスタ m 、判定回路 12、デクリメント回路 13 の各部品を共通に利用できる。新たに必要となる部品は、論理積回路 20 の一つだけである。

【 0 0 5 5 】

以下に、 $B \leftarrow A \times D$ を計算する乗算アルゴリズムを示す。

【 0 0 5 6 】

入力は、 A 、 D 、 G 、 m (G は m 次多項式、 A と D は次数が m より小さい多項

式)である。

【0057】

＜乗算アルゴリズム＞

パラメータの値の入力

B = 0

while m ≠ 0

 m ← m-1

 B ← twice(B)

 A ← left_shift(A)

 if msb(A) = 1 then B ← B xor D

wend

Bを出力する

＜乗算アルゴリズム＞

ところで、本実施形態のレジスタmとレジスタnをワンホットカウンタで実現することにより、入力は何ビットであっても全体として回路遅延が定数段となる逆元計算回路とすることができる。

【0058】

図10に、ワンホットカウンタの例を示す。

【0059】

ワンホットカウンタでは、m+1個のレジスタのうち1つだけある1が格納されたレジスタの番号で数表現する。図10では、番号2のレジスタに1が格納されているので数2を表現している。

【0060】

ワンホットカウンタでは、

- 1) 表現している数を1増やす操作は左シフトである、
 - 2) 表現している数を1減らす操作は右シフトである、
 - 3) 表現している数がある特定の数であるかどうかを判定するのは特定のビットが1であるかどうかを判定するだけでよい、
- という3つの特徴があり、これらのいずれの操作も回路遅延は定数段である。

【 0 0 6 1 】

さて、先に示した逆元計算アルゴリズム 1 やこれをフローチャートで表した図 1 は、種々変形して実施することが可能である。

【 0 0 6 2 】

以下では、先に示した逆元計算アルゴリズム 1 のループを一重にすることでハードウェア化しやすくした実施形態を示す。

【 0 0 6 3 】

この場合の逆元計算アルゴリズムを以下に示す。

【 0 0 6 4 】

< 逆元計算アルゴリズム 2 >

入力 A, B, G, m (G は m 次多項式、A と B は次数が m より小さい多項式)

C ← G

D ← 0

n ← 0

state ← 1

while m ≠ 0 and n ≠ 0

 f ← msb(A)

 if f = 1 then

 if state = 1 then

 (A, C) ← (A xor C, A)

 (B, D) ← (B xor D, B)

 else

 A ← A xor C

 B ← B xor D

 endif

 endif

A ← left_shift(A)

```

if state = 1 and (f = 0 or n = 0) then
    m ← m-1
    n ← n+1
    B ← twice(B)
else
    n ← n-1
    D ← half(D)
    if n = 0 then state ← 1 else state ← 0
endif
wend

```

Dを出力する

＜逆元計算アルゴリズム 2＞

以上のアルゴリズムの記述をフローチャートの形で表したのが図 1 1 である。

【0 0 6 5】

このアルゴリズム（逆元計算アルゴリズム 2）は、先に説明したアルゴリズム（逆元計算アルゴリズム 1）に比較して、state および f という 1 ビットの変数が増えている。途中で A が書き換わっているので、f は m s b (A) を保持しておくものである（ただし、ハードウェア化した際には必要なくなる）。state は、逆元計算アルゴリズム 1 の内側にある二つのループのいずれを回っているかを表している（状態を記憶しているので、ハードウェア化した際には記憶装置が必要になる）。f = 1 のときが最初のループ（step 1）と step 2 の状態にいて、f = 0 のときが後の方のループ（step 3）にいてることを示している。

【0 0 6 6】

この逆元計算アルゴリズム 2 についても、これをハードウェア化した際の構成は、図 7 と同じである。

【0 0 6 7】

また、この場合も、図 7 の部品を利用し、これに論理和回路 2 0 を追加して、図 9 及び前述の乗算アルゴリズムで示した乗算器が構成可能である。

【 0 0 6 8 】

なお、この逆元計算アルゴリズムの実行中の各レジスタの途中結果は、基本的には、図 6 と同様である。

【 0 0 6 9 】

また、逆元計算アルゴリズム 1，2 以外にも、それらと等価なアルゴリズムになるように、種々変形して実施することが可能である。この場合にも、これまで説明してきたと同様の作用効果を得ることができる。

【 0 0 7 0 】

なお、以上の各機能は、ソフトウェアとして実現可能である。

また、本実施形態は、コンピュータに所定の手段を実行させるための（あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための）プログラムとして実施することもでき、該プログラムを記録したコンピュータ読取り可能な記録媒体として実施することもできる。

【 0 0 7 1 】

なお、この発明の実施の形態で例示した構成は一例であって、それ以外の構成を排除する趣旨のものではなく、例示した構成の一部を他のもので置き換えたり、例示した構成の一部を省いたり、例示した構成に別の機能あるいは要素を付加したり、それらを組み合わせたりすることなどによって得られる別の構成も可能である。また、例示した構成と論理的に等価な別の構成、例示した構成と論理的に等価な部分を含む別の構成、例示した構成の要部と論理的に等価な別の構成なども可能である。また、例示した構成と同一もしくは類似の目的を達成する別の構成、例示した構成と同一もしくは類似の効果を奏する別の構成なども可能である。

また、この発明の実施の形態で例示した各種構成部分についての各種バリエーションは、適宜組み合わせて実施することが可能である。

また、この発明の実施の形態は、個別装置としての発明、関連を持つ 2 以上の装置についての発明、システム全体としての発明、個別装置内部の構成部分についての発明、またはそれらに対応する方法の発明等、種々の観点、段階、概念ま

たはカテゴリに係る発明を包含・内在するものである。

従って、この発明の実施の形態に開示した内容からは、例示した構成に限定されることなく発明を抽出することができるものである。

【 0 0 7 2 】

本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【 0 0 7 3 】

【発明の効果】

本発明によれば、標数 2 のガロア体での逆元計算アルゴリズムを V L S I 化した際、回路規模や回路遅延を従来よりも小さく抑えることができるようになる。

【図面の簡単な説明】

【図 1】

本発明の一実施形態に係る標数 2 の拡大体での逆元計算アルゴリズムの一例を示すフローチャート

【図 2】

同実施形態に係る多項式の表現について説明するための図

【図 3】

同実施形態に係る `left__shift` について説明するための図

【図 4】

同実施形態に係る `twice` について説明するための図

【図 5】

同実施形態に係る `half` について説明するための図

【図 6】

同実施形態に係る逆元計算アルゴリズムについて説明するための図

【図 7】

同実施形態に係る逆元計算アルゴリズムをハードウェア化した際の構成例を示す図

【図 8】

同実施形態に係る逆元計算アルゴリズムをハードウェア化した際の状態遷移の

一例を示す図

【図 9】

同実施形態に係る逆元計算アルゴリズムをハードウェア化した際の構成と大部分の部品を共通に利用できる乗算器の構成例を示す図

【図 1 0】

同実施形態に係るワンホットカウンタの例を示す図

【図 1 1】

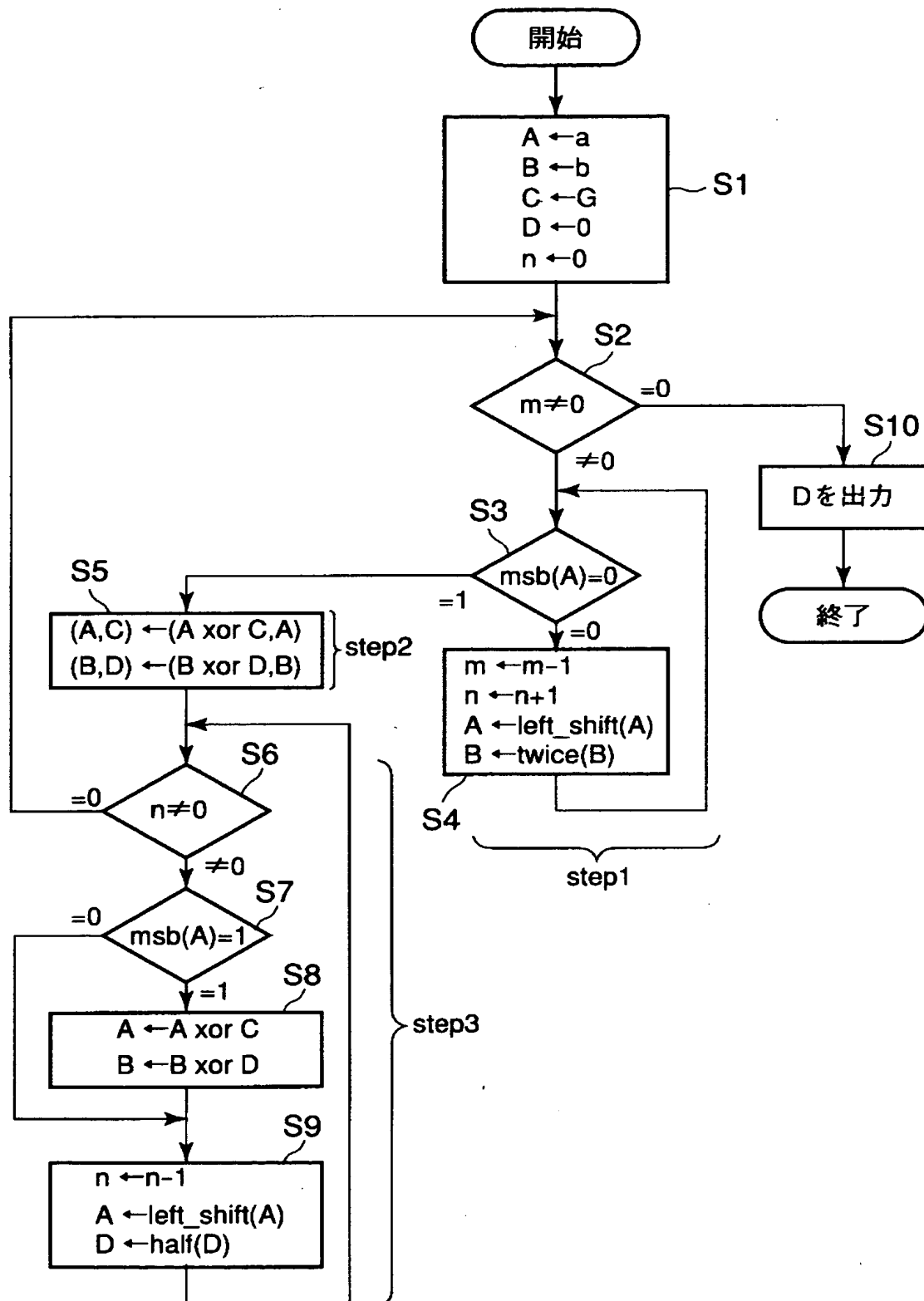
同実施形態に係る標数 2 の拡大体での逆元計算アルゴリズムの他の例を示すフローチャート

【符号の説明】

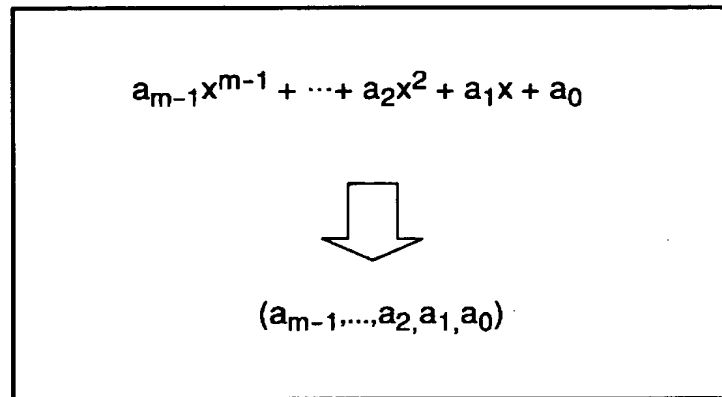
- 1 ～ 6 … レジスタ
- 7, 9 … 排他的論理和回路
- 8 … 左シフト回路
- 1 0 … 2 倍演算回路
- 1 1 … 1 / 2 倍演算回路
- 1 2, 1 4 … 判定回路
- 1 3 … デクリメント回路
- 1 5 … デクリメント回路
- 1 6 … インクリメント回路
- 2 0 … 論理積回路

【書類名】 図面

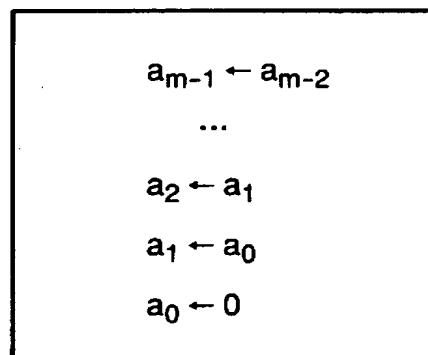
【図 1】



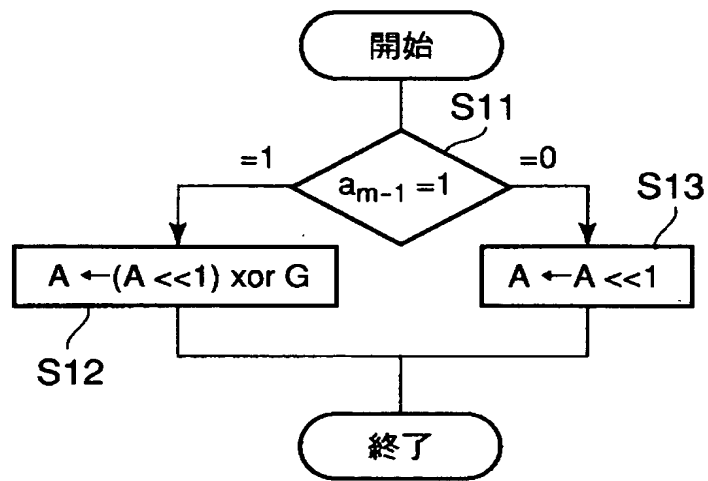
【図 2】



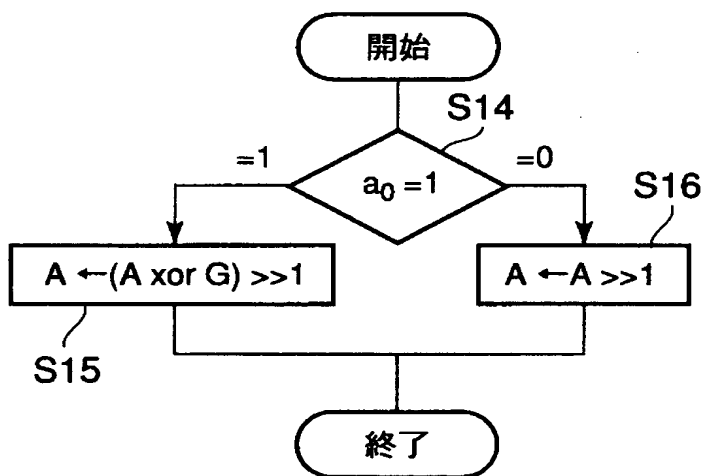
【図 3】



【図 4】



【図 5】

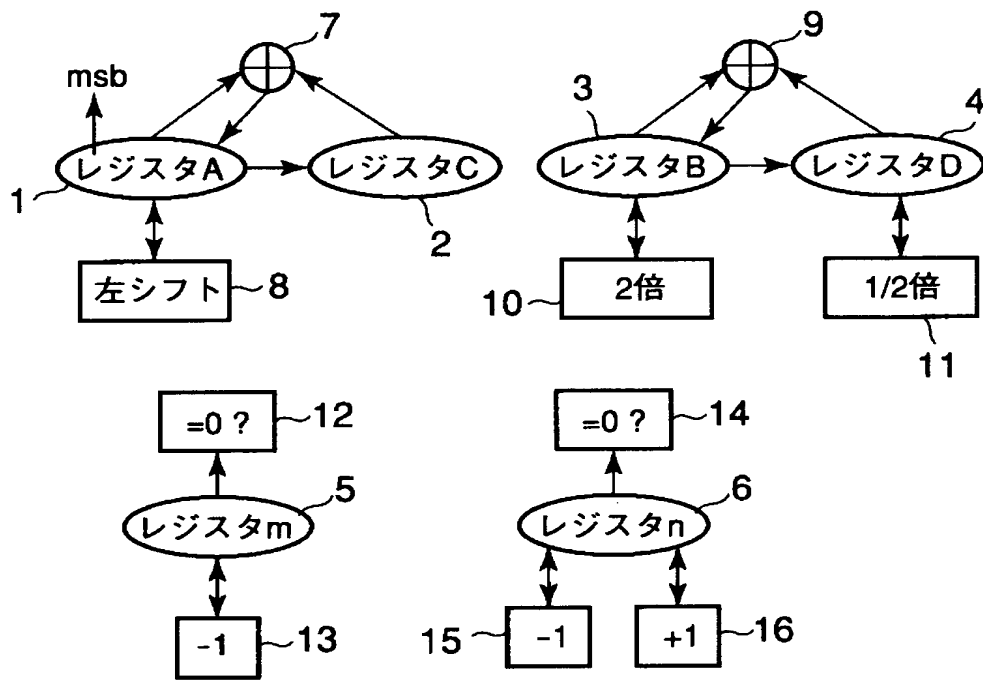


【図 6】

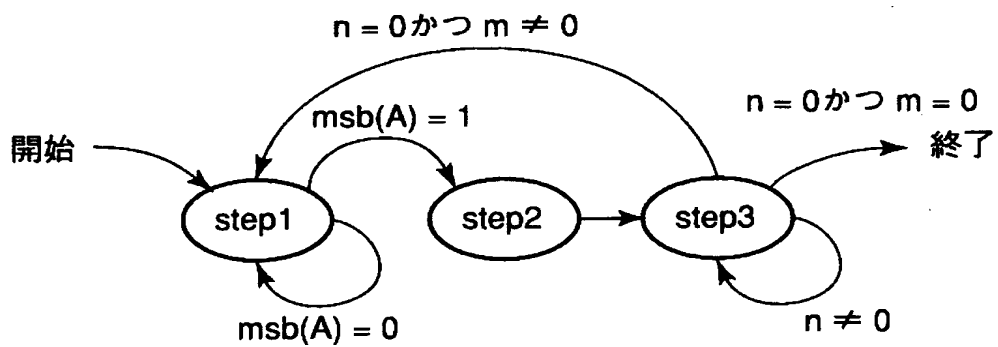
	A	B	C	D	m	n	step
0	<u>00011</u>	00001	<u>10011</u>	00000	4	0	
1	<u>00110</u>	00010	<u>10011</u>	00000	3	1	step1
2	<u>01100</u>	00100	<u>10011</u>	00000	2	2	
3	<u>11000</u>	01000	<u>10011</u>	00000	1	3	
4	<u>01011</u>	01000	<u>11000</u>	01000	1	3	step2
5	<u>10110</u>	01000	<u>11000</u>	00100	1	2	step3
6	<u>01110</u>	01100	<u>11000</u>	00100	1	2	(if成功)
6'	<u>11000</u>	01100	<u>11000</u>	00010	1	1	
7	<u>00100</u>	01110	<u>11000</u>	00010	1	1	(if成功)
7'	<u>01000</u>	01110	<u>11000</u>	00001	1	0	
8	<u>10000</u>	01111	<u>11000</u>	00001	0	1	step1
9	<u>01000</u>	01110	<u>10000</u>	01111	0	1	step2
10	<u>10000</u>	01110	<u>10000</u>	01110	0	0	step3

結果
 $(0,1,1,1,0)=x^3 + x^2 + x$

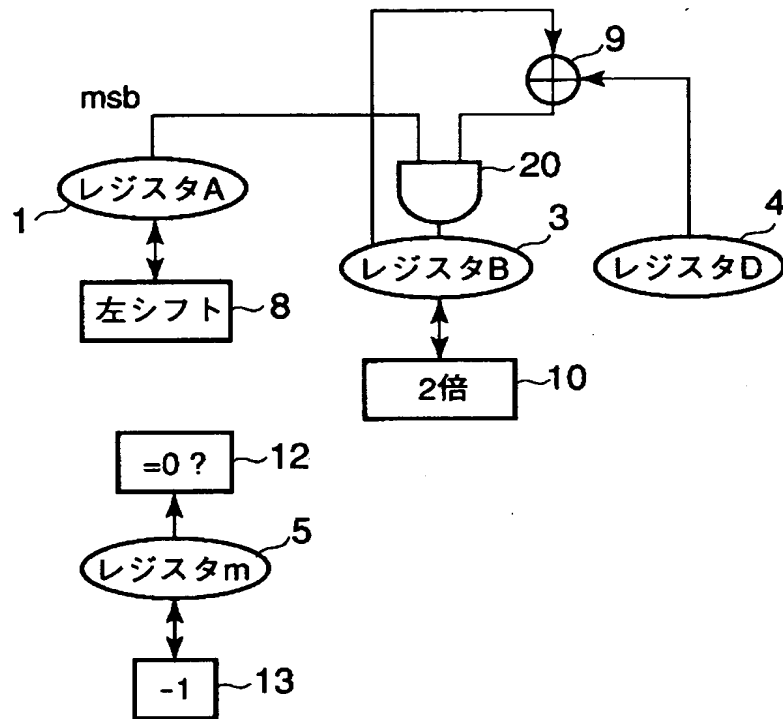
【図 7】



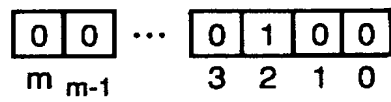
【図 8】



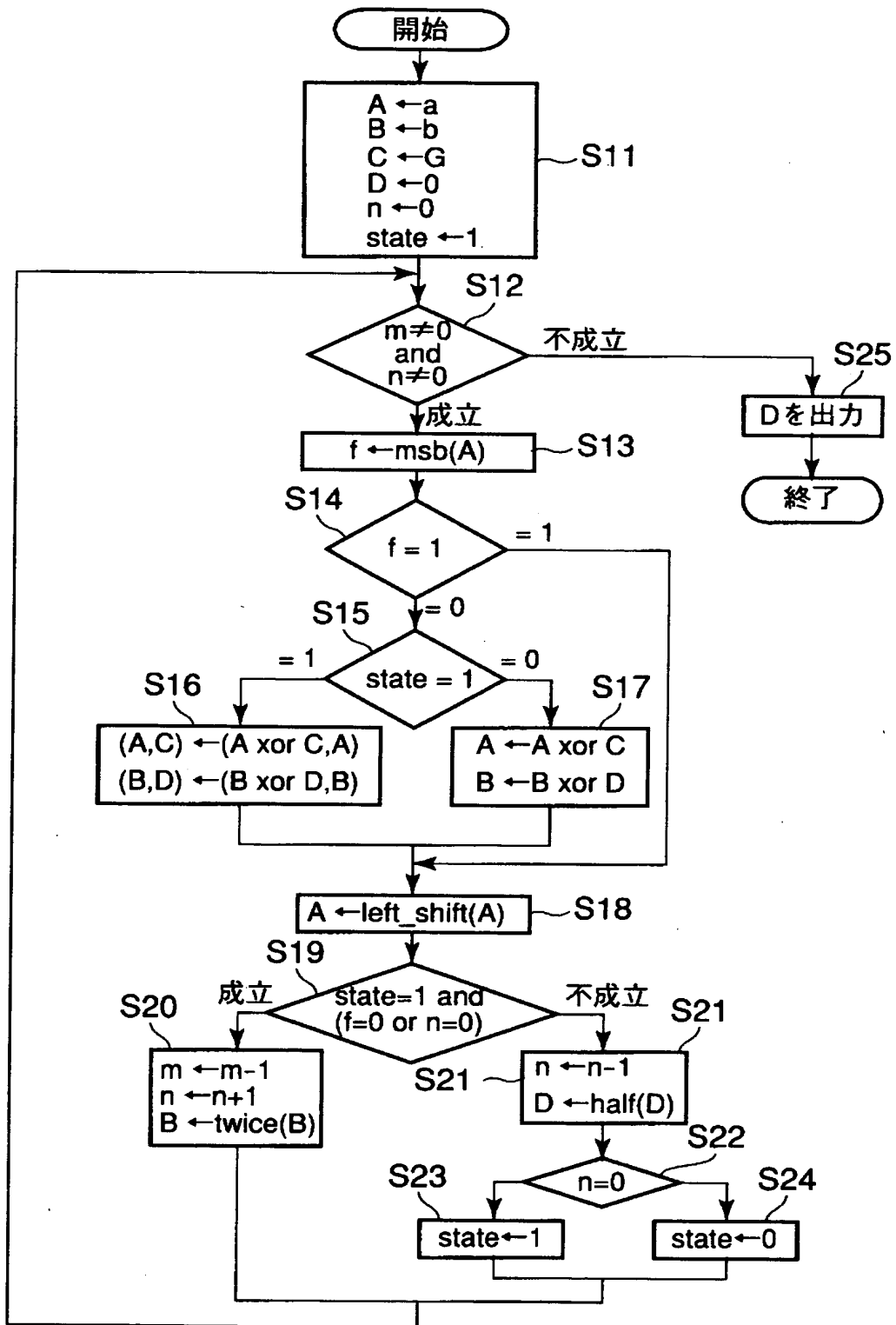
【図 9】



【図 1 0】



【図 11】



【書類名】 要約書

【要約】

【課題】 標数 2 のガロア体での逆元計算アルゴリズムを V L S I 化した際、回路規模や回路遅延をより小さく抑えられる逆元計算装置を提供すること。

【解決手段】 第 1 乃至第 6 のレジスタ（1 ～ 6）と、左シフト回路（8）と、排他的論理和回路（7， 9）と、標数 2 の拡大体での 2 倍演算を施す 2 倍演算回路（1 0）と、標数 2 の拡大体での $1/2$ 倍演算を施す $1/2$ 倍演算回路（1 1）と、レジスタの内容が 0 か否か判定する判定回路（1 2， 1 4）と、レジスタの内容をデクリメントするデクリメント回路（1 3， 1 5）と、レジスタの内容をインクリメントするインクリメント回路（1 6）と、それらを制御する制御回路とを用いて構成する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000003078]

1. 変更年月日	2001年 7月 2日
[変更理由]	住所変更
住 所	東京都港区芝浦一丁目1番1号
氏 名	株式会社東芝